2019全国CIO大会

新技术赋能业务新场景

信息安全建设规划实践

邢红波　前途汽车（苏州）有限公司

企业网D1Net 企业IT第1门户

信众智 CIO智力共享平台

目录
CONTENTS

PART 01

风险挑战

01 1.1 企业信息安全规划的背景

- **数字化转型企业需要对数字资产进行合理、有效的保护**
  - 随着企业数字化转型的深入，线上线下一体化“数字化双胞胎”运营的逐步实现，信息资产已经成为企业最有价值，最具竞争力的核心资产，如何理更合理、更高效实现信息（数字）资产的保护，是对信息安全建设提出更高要求。
- **工业互联网建设需要企业有与之匹配的安全管控能力**
  - 工业互联网时代IT、OT、CT快速融合，IoT模糊了传统安全边界，数据安全是工业互联网面临的最大壁垒之一，开展针对性的信息安全建设是构架坚固的网络安全系统、管理脆弱环节、保护敏感信息与知识产权的有效途径。
- **利益驱动下的信息安全事件频发给企业造成巨额经济损失**
  - 在当今信息即财富的背景下，越来越多的黑客组织投身于信息资产的窃取，攻击手段变幻莫测，而且攻击渠道日益变幻，IoT设备、工业网已成为不法黑客的攻击重点，为整个网络空间安全环境带来全新挑战。
- **数字化转型需要相应的信息安全管理体系及技术手段为企业合规运营保驾护航**
  - 国外GDPR、联邦数据法；国内安全法、工业控制系统安全防护指南、信息安全等级保护办法；企业需要通过ISO27001认证，建立相应的安全规划方案给后续的体系建设指明方向，确保企业合规运营。

01 1.2 信息安全建设风险和挑战

- 企业数据化转型的深入，传统意义上固定的安全边界已经消失，工业互联网、移动办公、云计算、IoT等使信息跨越了办公边界而自由流动；汽车的电动化、智能化、网联化、共享化趋势，使得新兴技术的发展应用在提高工作效率，满足客户体验同时，特别是政策性影响，也给安全技术带来了新的风险、挑战和要求

	数据保护	移动办公	云计算	安全运营中心
特点	▸ 数据无处不在，系统、终端、网络、手机等等 ▸ 知识共享与协同工作需要更频繁的数据交换 ▸ 社交媒体的蓬勃发展增加了数据传输的渠道	▸ 设备的类型多样化与可移动性增强 ▸ 网络接入渠道的增多与频繁的接断性 ▸ 移动应用的丰富化、个性化、定制化	▸ 基础架构投资的经济效益提升 ▸ 网络带宽的发展促进了多种模式的云服务 ▸ 资源的可扩展性与数据集中化管理	▸ 看不见、摸不着的未知安全攻防 ▸ 企业的安全健康状况难窥全貌 ▸ 总是在为扑救安全事件而买单
IT挑战	▸ 有效管理分散在各处的数据 ▸ 保障日渐庞大的数据的顺畅使用 ▸ IT消费品化、BYOD带来的设备管理多样化	▸ 标准化配置的综合管理 ▸ 远程设备的策略部署与平台化管理 ▸ 改造传统应用以适应于移动设备访问 ▸ 移动应用的定制化开发	▸ IT传统基础架构的转变 ▸ 从传统的外包服务转向云服务 ▸ 更弹性的负载均衡技术使用 ▸ 用户操作习惯的转变	▸ 多种异构设备的日志标准规范与统一 ▸ 海量日志的有效归并管理与压缩存储 ▸ 技术与管理的流程融合与决策支持
安全要求	▸ 识别整个企业中的敏感数据并进行分类分级 ▸ 从对渠道的关注转变为对数据内容的关注 ▸ 配套的管理制度须先行，保护策略须持续更新 ▸ DLP系统与其他控制措施的综合管控	▸ 移动设备自身的物理安全保护 ▸ 移动设备的普及要求加强对接入公司内部网络设备的认证管理 ▸ 移动设备的离线管理 ▸ 应对移动应用恶意代码的攻击	▸ 传统的基于物理边界的安全防护机制的转变 ▸ 对有权存取敏感数据的第三方给予特别关注 ▸ 从终端防护到更强的网络与服务端安全保护 ▸ 集中的用户、数据、应用带来更严重的攻击	▸ 安全健康状况的实时监控、预警和响应管理 ▸ 多系统日志的智能综合分析 ▸ 安全威胁的自动化评估 ▸ 以资产为核心，以业务系统为主线，量化企业风险等级

01 1.3 信息安全建设必要性和迫切性

企业信息安全需求

- **全球合规遵从**
  - 国内：网络安全法、等级保护、工业控制系统信息安全防护指南；
  - 国外：GDPR、联邦数据保护法；
  - 标准：ISO27001、ISA99
- **业务和产品安全**
  - 互联网业务系统安全
  - 车联网安全
  - 工控系统安全
  - 研发办公环境安全
- **数据资产保护**
  - 企业核心数据资产保护
  - 个人隐私信息PII保护
- **防黑客攻击**
  - 防渗透
  - 防病毒
- **系统可用性保障**
  - 办公网及生产网稳定性
  - 防DDOS攻击
  - 容灾备份

企业信息安全现状

- **信息安全管理**
  - 安全组织尚不完善
  - 安全管理制度和流程不完善
- **信息安全技术**
  - 已部署一部分安全技术方案缺乏系统全面的安全技术架构规划
  - 未执行网络隔离，缺乏桌面端防病毒软件，缺乏IT资产统一管理平台，缺乏设备准入控制，缺乏内网漏扫工具…
- **人员安全意识**
  - 人员信息安全意识不足
  - 员工的无意识的风险行为，可能为企业带来严重的信息安全损失
- **安全事件**
  - 勒索病毒事件/数据泄漏事件

01 1.4 企业信息安全风险项分析

编号	风险项	风险类型	风险等级	备注
1	信息安全组织缺失	管理风险	高	
2	信息安全管理制度缺失	管理风险	高	
3	员工安全意识不足	管理风险	高	
4	访客访问管理风险	技术风险	高	
5	终端安全管理风险	技术风险	高	
6	服务器安全管理风险	技术风险	高	
7	移动设备安全管理风险	技术风险	高	
8	网络访问安全管理风险	技术风险	高	
9	数据库安全管理风险	技术风险	高	
……	……	……	……	

PART 02

策略目标

02 2.1 企业信息安全建设策略

- 从企业战略和IT战略出发，设计企业信息安全建设整体策略

企业战略

IT战略

- 与公司战略保持一致
- 满足企业业务需求
- 体现信息部门的价值
- 符合相应行业法规要求

信息安全原则选择

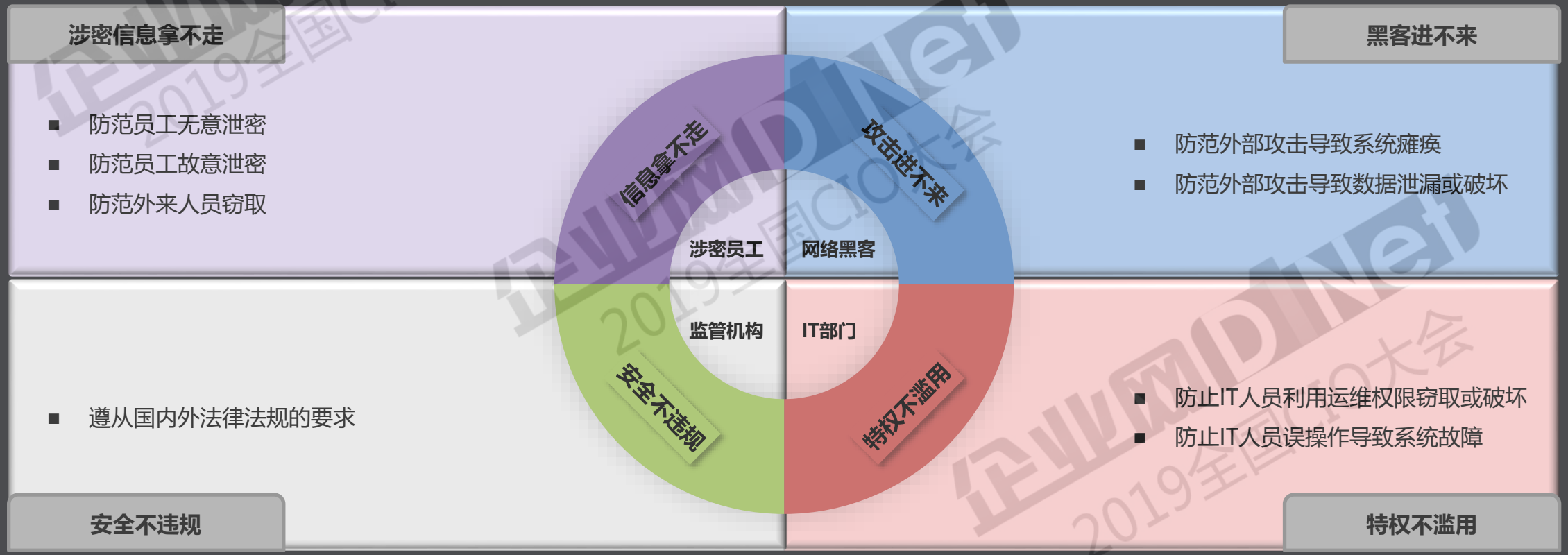
市场环境	VS	封闭环境
合规文化	VS	自由文化
注重隐私	VS	注重共享
面向业务	VS	独立建设
产品竞争	VS	运营竞争
安全优先	VS	效率优先
管理重要	VS	技术重要
预防为主	VS	事件驱动

信息安全策略

- 在保障企业正常运营效率的同时，采用一切必要的管理和技术手段，保护企业的核心数据资产和IT系统的机密性，完整性和可用性；
- 确保企业的信息安全运营符合相应法律法规的要求

02 2.2 企业信息安全建设目标

- 信息安全建设能够通过“人防+技防”实现“事前防范、事中控制、事后追溯”管理目标，全面降低企业信息安全风险，实现合规运营营。



PART 03

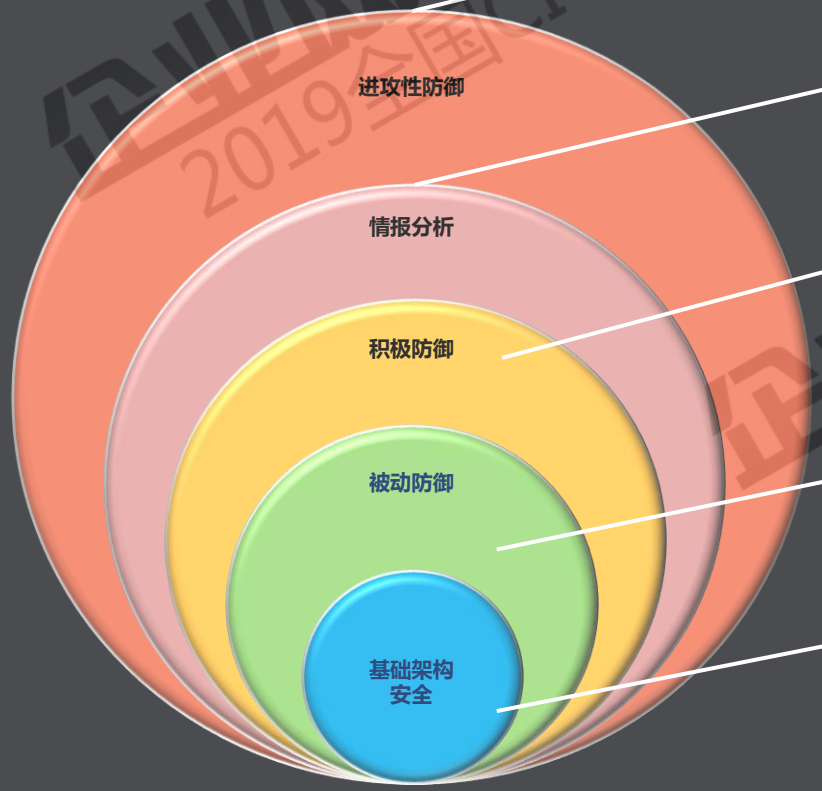
规划理念

03 3.1 企业信息安全建设的原则和策略

- 用信息安全成熟度滑动标尺模型为工具进行行业对标，确定信息安全建设中期目标（3年）

1.0 基础结构安全	2.0 被动防御	3.0 积极防御	4.0情报	5.0 进攻性防御
在系统规划，建立和维护的过程中充分考虑安全防护	在无人员持续介入的情况下，附加在系统架构之上可持续的威胁防御系统	分析人员监控和响应网络内部威胁并学习完善防御体系的过程	收集数据，将数据利用转换为信息，并将信息生产加工为评估结果，以填补已知知识缺口的过程	以法律反制措施等形式针对进攻者采取的自我防卫行动

03 3.2 行业对标



5.0 工作重心

- 安全实验室
- Built-in Security
- Script / SQL / SP白名单、运行时安全沙盒、标签数据流自动检测、LLVM容器级透明过滤、应用和系统安全内置

4.0 工作重心

- 认证鉴权中心
- Design for Security
- 应用接口认证鉴权、反汇编与攻击链分析、API接口地址偏移检测与分析、漏洞挖掘与分析

3.0 工作重心

- 安全运营中心、外部蓝军
- 大数据分析、服务器行为画像、专业蜜罐、生物认证、证书TPM保护、动态秘钥与加密机、黑产情报收集与分析
- ABAC访问控制、DevSecOps、安全自动化

2.0 工作重心

- 安全运维、应急响应团队
- 安全基线
- 企业级日志监控与分析SIEM、云服务安全策略强制网关CASB、打印监控、内容外传监控DLP、非法外连监控、渗透测试、漏洞扫描

1.0 工作重心

- 基本安全组织
- 安全红线
- 防毒软件、邮件网关、漏洞修复、防火墙、网络分区与隔离、IPS、WAF，

03 3.3 指导理念

- **信息安全建设指导理念：“P.P.T”（Process、Personal、Technology）**

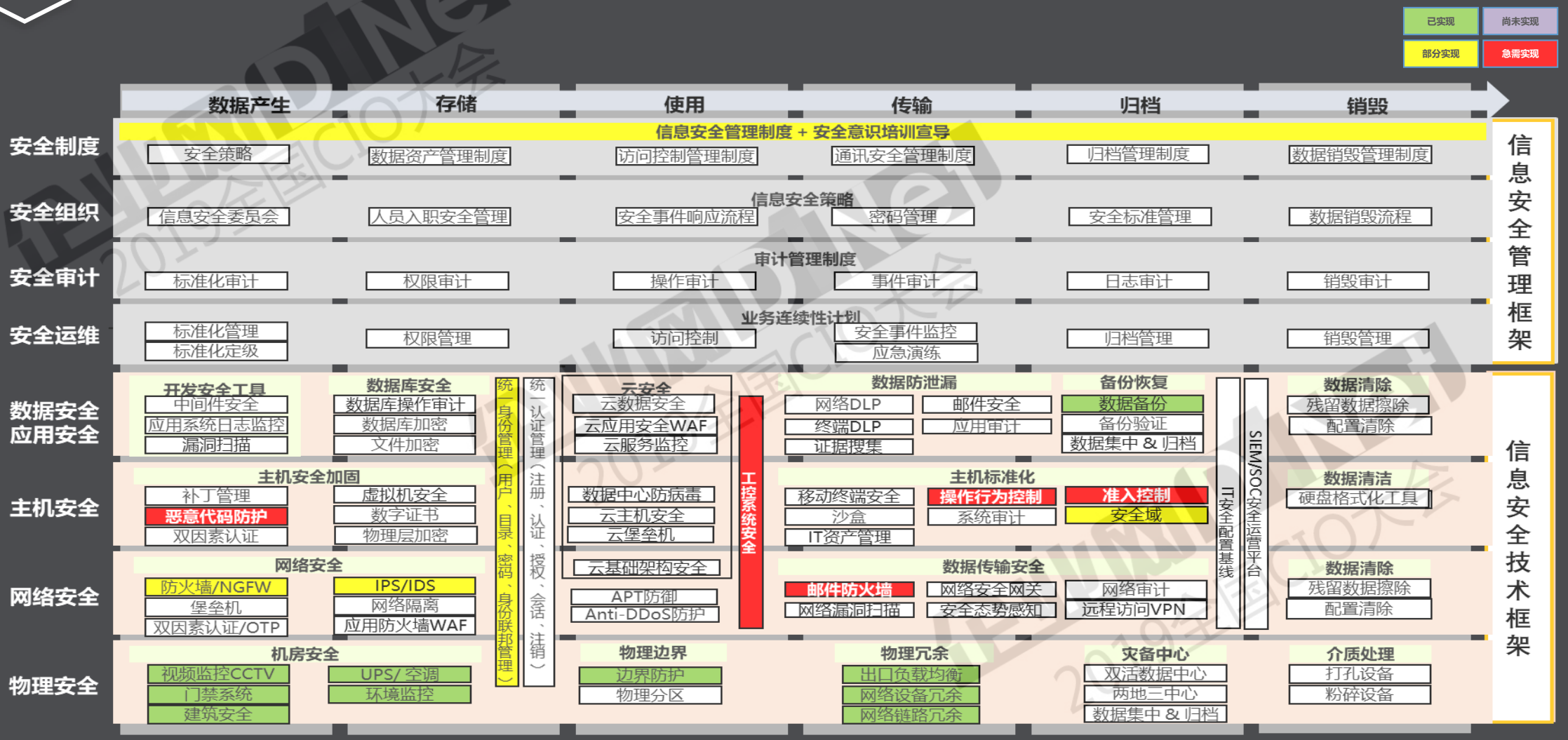
  - 信息安全工作，管理是核心，技术是手段，不是仅靠技术系统上线就可完成，而是融合管理和技术两方面的投入，进而改变员工的思想，行为和企业安全文化的一个持续过程

1. **程序**
   - 明确定义组织责任、策略要求、流程固化，构建信息安全建设的体系和运营基础。
2. **技术**
   - 对标信息安全建设最佳实践模型，定位企业在信息安全技术架构中的薄弱环节；
   - 分析技术系统部署优先级及关联性，确保关键信息安全风险的可发现，可控制，和可追溯审计。
3. **人员**
   - 采用教育和惩戒结合的方式，促进员工的信息安全意识，行为和文化的形成。

PART 04

实施模式

04 4.1 基于数据全生命周期的数据安全框架规划



04 4.2 技术能力实施路径图优先级思路

合理估算项目任务收益，确定合适的资源投入，提高工作效率

合理识别项目风险严重性，以定量的方式分析风险，有助于有针对性的控制项目整体风险

合理分析不执行项目任务存在的风险，明确项目任务存在的意义

通过对标最佳实践，保证项目实施的科学性，提高项目成功的概率

合理评估项目任务的易实施性并合理安排，有利于集中资源和精力攻克难题

04 4.3 建设步骤规划

04 4.4 建设内容实施规划

成熟度达到1.0 → 成熟度达到2.0 → 成熟度达到3.0

A. 基础保障

A.1 建立基本安全组织
1）正式发布信息安全组织
2）完善信息安全执行团队
3）展开信息安全培训和意识宣导

A.2 建立信息安全管理体系
1）建立信息安全管理制度
2）建立信息安全管理流程

A.3 防病毒项目
1）办公、生产、研发等环境全面部署防病毒软件。

A.4 网络准入控制
1）对接入公司网络的所有公司现有设备，新增设备，外来 人员设备进行认证管理，实行网络分区管理。

A.5 桌面标准化
1）对公司办公、研发、生产等所有终端实现桌面标准化管理，禁止员工私自安装软件

A.6 域控管理
1）对公司所有人员实行域控管理。

A.7 外部网络安全
1）部署互联网边界防火墙隔离内外网；
2）部署IPS/NGFW/WAF全面防御网络攻击

A.8 邮件安全
1）部署邮件网关，控制垃圾邮件及钓鱼邮件的风险；

B. 纵深防御

B.1 完善信息安全组织
1）建立符合国际标准的完善的信息安全组织
2）构建信息安全团队，强化安全策略能力

B.2 信息安全管理体系项目
1）以ISO27001\等保为框架构建信息安全管理体系；
2）通过ISO27001\等保信息安全管理体系认证。

B.3 数据防泄漏（DLP）
1）部署终端、网络、邮件数据防泄漏系统，建立数据资产安全管理制度和使用流程。

B.4 内网络隔离项目
1）部署研发网、办公网，数据中心隔离防火墙，隔离内网不同业务环境。

B.5 数据库审计
1）实现数据库日志、网络流量和访问的安全审计
2）对违规事件的基本的安全响应。

B.6 工控系统安全
1）实现对车间工控网的安全保护。

B.7 资产和漏洞管理平台
1）构建资产和漏洞扫描平台；
2）配置安全基线，对各业务系统的健康状况实时监控。

C. 安全运营

C.1 建立信息安全运营中心
1）建立安全运营中心，24*7的监控企业发生的安全事件并进行应急响应。

C.2 信息安全管理体系优化项目
1）编制信息安全技术手册（蓝皮书）；
2）部署和强制执行信息安全技术标准。

C.3 网络安全等级保护项目
1）备案核心业务系统，通过网络安全等级保护认证。

C.4 威胁情报中心项目
1）收集国内外威胁情报汇总成前途威胁情报池；
2）通过通用接口将威胁情报共享给各安全单元。

C.5 业务情报中心项目
1）建立业务情报数据，明确关键业务活动和数据的清单和位置；
2）针对是别的关键业务数据进行强化保护。

C.6 资产情报中心项目
1）识别关键业务活动对应的软、硬、人、服务等资产；
2）针对关键资产进行强化安全保护。

C.7 企业数字证书管理中心项目
1）建立企业级的密钥和证书管理平台；
2）自动产生、分发、更新和撤销企业数字证书和密钥。

04 4.5 “基础保障”能力建设规划实施项目及预算

项目编号	项目名称	部署范围和规模	建设模式	选型（方案/产品）	预算	备注
A.1	信息安全组织建立		自主建设			
A.2	信息安全制度和流程建立		自主建设/外部支持			
A.3	防病毒项目		外部支持			
A.4	网络准入控制项目		外部支持			
A.5	桌面标准化项目		自主建设			
A.6	域控管理		自主建设/外部支持			
A.7	外部网络安全		外部支持			
A.8	邮件安全		外部支持			
……	……	……	……	……	……	……

04 4.6 “纵深防御”能力建设规划实施项目及预算

项目编号	项目名称	部署范围和规模	建设模式	选型（方案/产品）	预算	备注
B.1	完善信息安全组织		自主建设			
B.2	信息安全管理体系项目		自主建设/外部支持			
B.3	数据防泄漏（DLP）项目		外部支持			
B.4	内网络隔离项目		外部支持			
B.5	数据库审计		外部支持			
B.6	工控系统安全		外部支持			
B.7	资产和漏洞管理平台		外部支持			
……	……	……	……	……	……	……

04 4.7 “安全运营”能力建设规划实施项目及预算

项目编号	项目名称	部署范围和规模	建设模式	选型选型（方案/产品）	预算	备注
C.1	信息安全运营中心		自主建设/外部支持			
C.2	信息安全管理体系优化		自主建设/外部支持			
C.3	网络安全等级保护项目		外部支持			
C.4	威胁情报中心		外部支持			
C.5	业务情报中心		外部支持			
C.6	资产情报中心项目		外部支持			
C.7	企业数字证书管理中心		外部支持			
……	……		……	……	……	……

结束语

信息安全问题，归根结底是人的问题；信息安全管理是“核心”，“技术”手段；“道高一尺，魔高一丈”，信息安全建设对只有起点，没有终点，我们永远在路上！

2019全国CIO大会

新技术赋能业务新场景

感谢聆听！

企业网D1Net 企业IT第1门户

信众智 CIO智力共享平台